

SaaS Security

BY



WHITEPAPER



"Financial institutions have become more open to SaaS cloud services. They recognize it as a differentiator"

INTRODUCTION

Historically, there was a view among financial institutions that data must be kept inside “the perimeter” of their organization. When **SaaS (software-as-a-service)** was introduced to the market, it was viewed as new, untested and potentially insecure. The risks were considered too high and, at the outset, only a small proportion of the sector integrated SaaS into their IT Ecosystem.

In recent times, financial institutions have become more open to **SaaS cloud services**. They recognize it as a differentiator to drive efficiencies and deliver on banking customer expectations in a rapidly changing fintech industry.

Pulsate examines why financial institutions were traditionally hesitant to make the transition from more conservative IT infrastructure to SaaS, the practical benefits associated with embracing SaaS, and how **Pulsate secures fintech data** through its cloud-based platform.

The information contained in this whitepaper is for information purposes only.
For specific advice, contact Pulsate directly at info@pulsate.com

Financial institutions move from traditional IT infrastructure to SaaS

In the past 10 years, more and more financial institutions are embracing software-as-a-service (SaaS) cloud services, despite initial reservations. Their reluctance was due to three main and very real concerns – regulations, risk and data breaches.

Regulation

There are stringent laws relating to information security. As financial institutions operate across different states, data needs to be stored according to the specific regulations in each jurisdiction.

Risk

In the early days of SaaS, security was difficult to define, therefore storing data in the cloud was deemed too risky by financial institutions.

Data breaches

All organizations, irrespective of the industry, are conscious of the repercussions of a data breach, not least the damage it would cause to their brands or reputation. When it comes to the banking sector, there is an added layer – **financial data is one of the most sensitive types of data**. Financial institutions have a duty of care to their customers and their customers' data. It needs to be protected without question.



Given the complexity of transitioning to SaaS, many financial institutions were reluctant to change until their fears were allayed. Yet, as the **economic and social needs of banking customers evolved**, change and the move to SaaS became inevitable.

Banking customers today expect to be able to pay bills, arrange a loan, receive advice and self-manage their banking online. As **fintech technology** becomes more customer-facing, financial institutions are tasked with protecting customer data online to counteract potential risks. There are stringent laws relating to information security. As financial institutions operate across different states, data needs to be stored according to the specific regulations in each jurisdiction.



How SaaS evolved for financial institutions

The cloud has evolved in the past decade. Before then, organizations strived to understand how to securely design and build different cloud services. Understandably, due to the sensitivity of the data they process, financial institutions were reluctant, at first. Early adopters tested cloud services and identified any issues, such as ill-defined security, enabling SaaS companies to troubleshoot and develop more sophisticated systems.

As **cloud services have matured** and initial issues were overcome, the **result is secure cloud platforms** with layers of controls in place and multiple accreditations to support it.



"The fundamental benefit of cloud and SaaS is the fast pace that they allow enterprises to build and launch products"

There is now trust in cloud platforms and, in turn, confidence amongst fintech companies. Financial institutions that were, in the early days, hesitant, have seen how their competitors have benefited from integrating SaaS into their systems. SaaS is built on top of cloud platforms, such as AWS, GCP and Azure. SaaS products leverage the native cloud security controls at different layers along with their own application layer security controls to give a well-defined, secure perimeter, which can match or exceed the security on a traditional on-premise network.

The fundamental benefit of cloud and SaaS is the fast pace that they allow enterprises to build and launch products. Many financial intuitions, who were traditionally risk-averse, now recognize that they need to be at the same pace, technically and functionally, as fast-paced fintech companies, such as the new generation cloud neobanks.

Financial institutions are recognizing that, in addition to protecting customer data, there are many benefits to working with companies that provide SaaS products and have secure cloud storage.

Practical benefits for financial institutions embracing SaaS



Cost effective

A cloud network is an operating expense (**opex**) rather than a capital expense (**capex**). It is required to facilitate SaaS cloud services. As **with all SaaS products, there is a shared cost for the service**. Ultimately, each financial institution pays only a fraction of what it would cost to build their own cloud network.



Lower operational overheads

With one less system to run, **financial institutions that engage with fintechs have less operational costs**. With SaaS, there are no installation or hardware costs; the saving is transferred to the customer.



Increased product development

The growth of SaaS for financial institutions was inevitable. With smaller start-ups disrupting the space, **fintech needs to be innovative and agile**. SaaS creates a platform for multiple end users. Instead of each financial institution having to create their own products, fintech companies are innovating on their behalf, without delay.



Greater security

In practice, data stored in **the cloud has less exposure to risks than physical networks** – when there are robust cybersecurity systems in place.



"In the fast-paced fintech space, financial institutions are using the Pulsate cloud platform to proactively communicate with their customers and nurture meaningful relationships in real-time"

How Pulsate secures fintech data

In the fast-paced fintech space, financial institutions are using the Pulsate cloud platform to proactively communicate with their customers and nurture meaningful relationships in real-time. This is facilitated by a host of communication activities made possible by push notifications, in-app messaging, geofencing, beacons, mobile feeds, SMS and email. This gives financial institutions large autoscaling and processing capabilities to deliver over **100,000** campaigns in minutes.

How is this data protected?

Pulsate leverages data security controls, such as encryption in transit (**TLS V1.2**), encryption at rest (**AES 256**), and defence in-depth network security. It is fully monitored with strict access controls in place and, due to multi data centre architecture, is highly available.

Pulsate is fully compliant with the **General Data Protection Regulation (GDPR)** with robust data protections controls, processes and policies in place.

Pulsate API provides developers with full functionality to push data and pull data from the platform, making integrations easy, securely.



CONCLUSION

Traditionally, financial institutions kept everything inside the perimeter behind the firewall. Inside this perimeter was the operating plane, robustly protecting their data. This system presented two key operational issues – it was expensive to ensure the data was accessible and making the data available to external stakeholders was complex. This posed a security risk to the entire network, which, in turn, required more stringent controls within the organization. With the multiple layers of bureaucracy came limitations in terms of moving or accessing data.

With SaaS, not only can data be moved, it is accessible and in line with the fast-paced nature of the industry.

Financial institutions now have segments of their data available across the cloud for different purposes. Risk is delegated; controls are more robust; there are multiple layers of security; and data access is well-protected.

Cloud-based virtual networks are scalable by default, monitored and highly available across multiple data centres.

Pulsate is a cloud-based marketing platform that enables financial institutions to proactively communicate with customers in real-time. Its technology enables financial institutions to maintain and strengthen the relationship with their banking customers across the US.

By leveraging behavioral and location data, they deliver personalized offers and time-sensitive information. Throughout the Covid crisis, Pulsate has helped community banks and credit unions to engage their most at-risk members and ensure they have access to financial support and digital services when they need it.

Founded in 2014, Pulsate is driving the transformation of marketing in retail banking to support the continued growth of community banking institutions in an increasingly digital world.

"Its (Pulsate) technology enables financial institutions to maintain and strengthen the relationship with their banking customers across the US"

Web: www.pulsatehq.com

Email: info@pulsatehq.com

Tel.: +353 (0)1 5240402

